**The Trojan Horse.**

The Trojan Horse recieved its name from the Legend of the Trojan War. It is a piece of software designed to work in a concealed manner, so you think it is doing one thing, when it actually is doing another.

It is important to note that a Trojan Horse is not a virus, for it does not replicate itself as viruses do. Instead it could be useful, for example, when you need to administer your server remotely. However, due to its often destructive capabilities, and designed to be malicious, it is considered to be a virus.

A non-malicious Trojan Horse may be used for remote access, remote managing, security software, and forensics.

Malicious Trojans gain access to your machine to perform harmful tasks. Trojans can be used for many things, such as gaining personal information from your computer, such as addresses, credit card information and passwords. They can be used to spy on you, delete or change files on your system. They can also be used to damage your hardware. Most attackers know that it is easy to discover a virus from its name, and so most attackers hide the virus in a program which you might think is useful, when in fact it is not. The Trojan horse camouflages itself so it appears as part of the system

You may download Trojans through a number of ways.

1. Software downloads
2. Websites containing executable content
3. Email attachments
4. Application exploits, for example, flaws in a web browser, media player, messaging client etc

Trojans can be removed through Anti viruses that have software designed to identify and delete the Trojan from your system. However, you do not know what effects the Trojan has had on your computer, or whether a hacker has retrieved information.

Some ways you may avoid catching a Trojan Horse include:

1. Do not download files blindly from people or sites you are not sure about.
2. Watch out for hidden file extensions. They are normally hidden extension files such as the file .exe extension, however, most hackers are aware of this, and so try to hide the name of the file so that you may not immediately realize what type of file you are using.
3. Do not always rely on your anti virus and think you are safe because you have one. Your anti virus has to be designed to detect Trojans.
4. Use an internet firewall